



Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0

First Published: 2021-03-25

Last Modified: 2022-01-13

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Planning 1

- Cisco Jabber Softphone for VDI 1
- Cisco Jabber and VDI 1
- The User Experience 4
- General Requirements 4
 - Accessories 5
 - Cisco Jabber for Windows 5
 - Cisco Unified Communications Manager 5
 - Cisco Expressway for Mobile and Remote Access (MRA) 5
 - Connection Broker—Installed on the Hosted Virtual Desktops 5
 - Operating Systems—Installed on the Hosted Virtual Desktops 6
 - Server Operating Systems—Installed on the Hosted Virtual Desktops 6
 - Port Requirements 6
 - Supported Codecs 7
- Requirements—HP Thin Pro 7
- Requirements—MacOS 8
- Requirements—Ubuntu 9
- Requirements—Unicon eLux 10
- Requirements—Windows 11

PART I

Deployment 15

CHAPTER 2

Deployment Overview 17

- Deployment Overview Workflow 17

CHAPTER 3

Downloads 19

Download the Cisco JVDI Agent 19
 Download the Cisco JVDI Client 19
 Download Cisco AnyConnect—Unicon eLux 20

CHAPTER 4 **Installation 21**

Set up the Hosted Virtual Desktops Workflow 21
 Install the Components Workflow—HP Thin Pro 22
 Install the Components Workflow—MacOS 23
 Run the MacOS Installer 23
 Accept permissions 23
 Install the Components Workflow—Ubuntu 24
 Install the Components Workflow—Unicon eLux 25
 Install the Components Workflow—Windows 26
 Cisco JVDI Client Installation 26
 Run the Microsoft Installer 27
 Use the Command Line 27
 Use the Group Policy Editor 27

CHAPTER 5 **Configuration 29**

Configuration Files 29
 Set up Users on the Cisco Unified Communications Manager Workflow 29
 Create a CSF Device and a Directory Number for Each User 30
 Associate New Devices with a User 32
 Enable the CTI Protocol for Users 32
 Configure Cisco Unified Communications Features for Users 33
 Change a User Password 33

CHAPTER 6 **Upgrade 35**

Upgrade Notes 35
 Version Support Strategy 35
 Upgrade Workflow 36

PART II **Troubleshooting 39**

CHAPTER 7	General Troubleshooting	41
	Problem Reporting Tool	41
	Virtual Channel Problem	42
	Configuration Files	42
	Verify That Cisco JVDI Agent Is Installed	42
	Verify Device Registration with Cisco Unified Communications Manager	43
	Verify the Connection Status in Cisco Jabber	43
	Jabber VDI Fallback Mode	43
	Disable BFCP desktop share	44

CHAPTER 8	Troubleshooting—HP Thin Pro and Ubuntu	45
	Verify the Platform Version—HP Thin Pro	45
	Verify the Platform Version—Ubuntu	45
	Verify That the Cisco JVDI Client Is Installed	46
	Verify That VXC Is Running on the Thin Client	46
	Call Control Is Lost After a Network Failure	46
	Call Is Lost After HVD Disconnection	47

CHAPTER 9	Troubleshooting—Unicon eLux	49
	Verify the Platform Base Image Version	49
	Verify That Cisco JVDI Client Is Installed	49
	Verify That VXC Is Running on the Thin Client	49
	Call Control Is Lost After a Network Failure	50
	Call Is Lost After HVD Disconnection	50

CHAPTER 10	Troubleshooting—Windows	51
	Configuration Files	51
	Registry Keys	51
	Verify That Cisco JVDI Client Is Running	52
	Confirm the Version of Cisco JVDI Client	52
	Call Control Is Lost After a Network Failure	52
	Call Is Lost After HVD Disconnection	53
	Enable Log Collection	53

Enable Memory Dump Collection 53

Display issues 54



CHAPTER 1

Planning

- [Cisco Jabber Softphone for VDI, on page 1](#)
- [Cisco Jabber and VDI, on page 1](#)
- [The User Experience, on page 4](#)
- [General Requirements, on page 4](#)
- [Requirements—HP Thin Pro, on page 7](#)
- [Requirements—MacOS, on page 8](#)
- [Requirements—Ubuntu, on page 9](#)
- [Requirements—Unicon eLux, on page 10](#)
- [Requirements—Windows, on page 11](#)

Cisco Jabber Softphone for VDI

The applications in the Cisco Jabber Softphone for VDI family of products are:

- Cisco Jabber Softphone for VDI—HP Thin Pro and Ubuntu
- Cisco Jabber Softphone for VDI—MacOS
- Cisco Jabber Softphone for VDI—Unicon eLux
- Cisco Jabber Softphone for VDI—Windows
- Cisco Jabber Softphone for VDI—Dell Wyse Thin OS (Available from, and supported by Dell Wyse)

Cisco Jabber and VDI

Cisco Jabber chat and presence are supported in Virtual Desktop Infrastructure deployments. However, because of a limitation known as the *hairpin effect*, calling and video capability are not supported. The additional bandwidth required for calls and video creates a bottleneck at the data center.

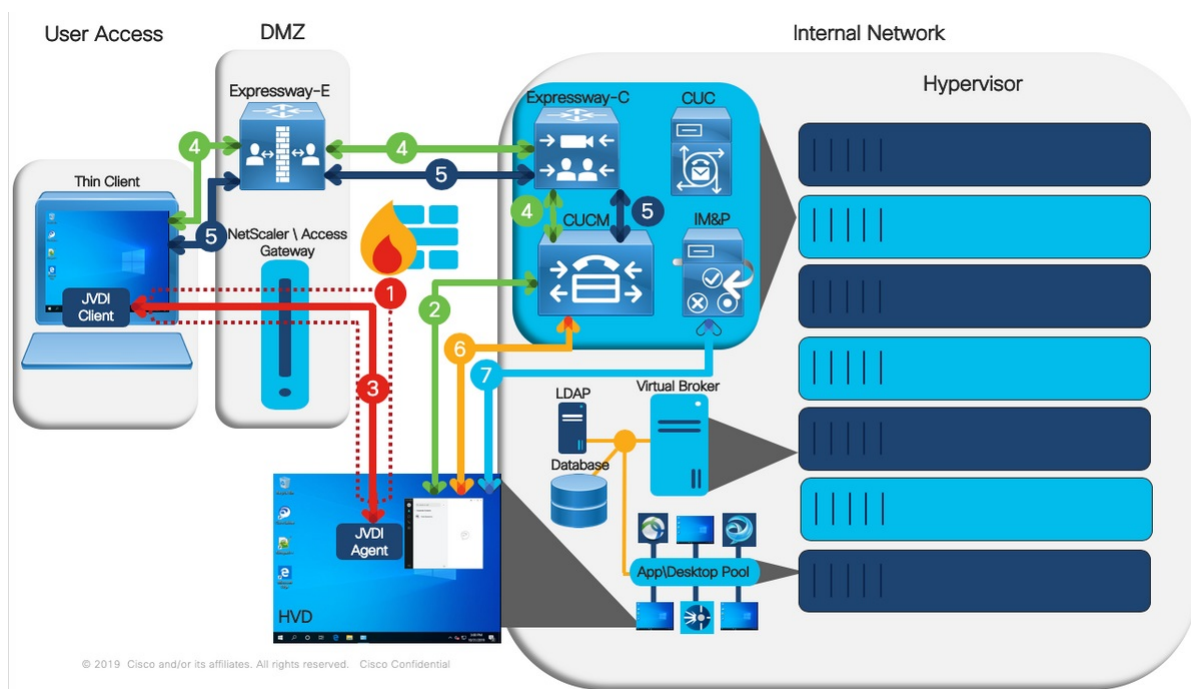
Cisco Jabber Softphone for VDI extends the Cisco collaboration experience to virtual deployments. With a supported version of Cisco Jabber for Windows, users can send and receive phone calls on their hosted virtual desktops (HVD). The Cisco Jabber Softphone for VDI software automatically detects the virtual environment. To reduce latency and to enhance media quality, Cisco Jabber Softphone for VDI streams media between the endpoints without going through the hosted virtual desktops.

The Cisco JVDI architecture consists of two primary components: the Cisco JVDI Agent and the Cisco JVDI Client. The Cisco JVDI Client is installed on a thin client while the Cisco JVDI Agent is installed on the HVD.

When a user launches a virtual broker client (Citrix Workspace app or VMWare Horizon Client), the software initiates a virtual channel. The JVDI Client and Agent use this virtual channel to communicate.

The diagrams below shows the architecture as well as the expected protocol sessions that are set up during normal use. In this example, Jabber is deployed in full UC mode over Mobile Remote Access (MRA). The next diagram shows the data flow between all components in a standard Cisco Jabber Softphone for VDI deployment.

Figure 1: Cisco Jabber Softphone for VDI—Architecture and Protocol Sessions



1. To start a session, users launch their virtual broker client (Citrix Workspace App or VMware Horizon Client) and connect to the connection broker and select a HVD or virtual application. Once select, a virtual channel is set up between the users' Thin Client (Physical Machine) and the HVD (Virtual Machine) hosted on the Hypervisor.
2. Once Jabber determines if it is in a virtual environment, the JVDI Agent process (hvdagent.exe) starts and begins the service discovery. Once authenticated with Unified CM, Jabber performs all its normal UDS queries (Home Cluster, UDS Server, Unified CM End User, and Device lookup) and caches all the retrieved information.
3. The JVDI Client and JVDI Agent then go through the process of setting up all the control streams that are used to exchange data over the virtual channel. Once these channels are set up, Jabber retrieves the cached information (Email Address, Voice Service Domain, Credentials, TFTP Server, Device Name, CTL Info, and LSC Info) and provides it to the JVDI Client.
4. The JVDI Client performs service discovery. It references either or both the cached email address (entered on Jabber login) and the voice service domain information that the JVDI Agent provided. The JVDI Client is able to resolve the _collab-edge DNS SRV record because this connection is over MRA. Once service

discovery is complete, the JVDI Client attempts to retrieve the CSF Device configuration, Application Dial Rules, and Directory Lookup Dial Rules from Unified CM TFTP through the Expressway.

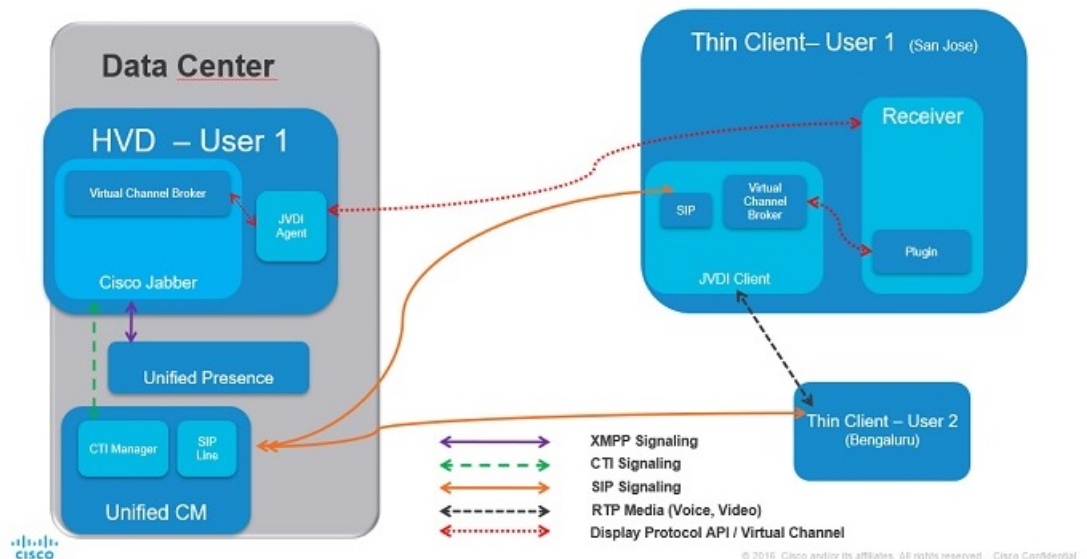
5. After receiving the CSF device configuration, the JVDI Client begins softphone registration process by performing the SIP registration process with the Unified CM CallManager services. Once completed, the CSF device shows as registered in the Cisco Unified CM Administration interface.
6. Jabber attempts to CTI control the registered CSF device. Jabber establishes a CTI QBE control session between the Jabber device and the Unified CM CTIManager service. When completed successfully, Jabber gains CTI control of the CSF device and line. This step enables Jabber to be able to make and receive calls.
7. The XMPP connection between Jabber and IM and Presence does not traverse the virtual channel. All XMPP traffic remains on the LAN directly between the HVD and the IM and Presence server.



Note

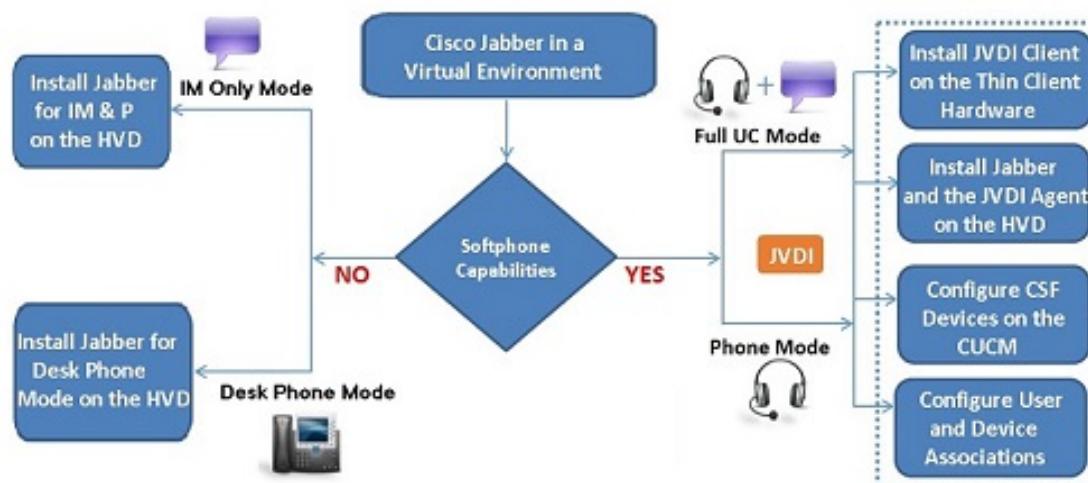
- JVDI over MRA does not support collab-edge SRV being resolveable from the hosted virtual desktop (HVD).
- For MRA deployments with Split DNS, the HVD must not discover the external domain. Do one of the following:
 - Configure SERVICES_DOMAIN and VOICE_SERVICES_DOMAIN during Jabber software installation on the HVD.
 - Configure servicesDomain and voiceServicesDomain parameters in the jabber-config.xml file.

Figure 2: Cisco Jabber Softphone for VDI—Data Flow



Use the following flowchart to determine whether you require Cisco Jabber Softphone for VDI.

Figure 3: Do You Need Cisco Jabber Softphone for VDI?



The User Experience

Cisco Jabber Softphone for VDI detects the virtual environment at run time and Cisco Jabber starts in virtualization mode. The user experience with Cisco Jabber for Windows and Cisco Jabber Softphone for VDI is similar to the non-VDI experience. However, in a virtual environment there are some minor differences:

- **Device Selector**, which is located in the Windows notification area, allows users to quickly switch their active camera and audio devices. Device management is also available from within Cisco Jabber.
- **Headset Priority**—By default, Cisco Jabber adds a newly connected device to the top of the priority list, and makes the new device active. You can set the `HeadsetPreference` parameter so that Cisco Jabber adds new devices to the bottom of the priority list. For more information, see *Parameters Reference Guide for Cisco Jabber*.



Note Users can override this setting in their **Audio** preferences.

- **Feature Support**—Cisco Jabber Softphone for VDI supports most Cisco Jabber for Windows features, with some exceptions. For more information, see the notes for your platform in [Release Notes for Cisco Jabber Softphone for VDI](#).

General Requirements

General requirements apply to all Cisco Jabber Softphone for VDI platforms.



Important

Only the components, versions, and minimum hardware requirements listed in this guide are supported. Use of unsupported components can result in a nonfunctional deployment.

Accessories

For a complete listing of recommended audio and video accessories, see *Unified Communications Endpoint and Client Accessories*, at http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html.

Ensure that all Jabra devices are running the latest firmware. You can use Jabra Direct to update the firmware.

Cisco Jabber for Windows

This release of Cisco Jabber for Windows, running on the hosted virtual desktop (HVD).

For complete information about virtual environment compatibility, see the Cisco Jabber documentation for your release.

Cisco Unified Communications Manager

Recommended: Unified CM Release 11.5(1)SU3 or later

Minimum: Unified CM Release 10.5

Cisco Expressway for Mobile and Remote Access (MRA)

Recommended: Expressway X12.5

Minimum: Expressway X8.11.4

Cisco Jabber Softphone for VDI with MRA only supports OAuth 2.0 for authentication. See the [Deploying OAuth with Cisco Collaboration Solution](#) guide for more information.



Note JVDI over MRA does not support collab-edge SRV being resolveable from the HVD. Softphone registration with JVDI fails in this case.

When using JVDI over MRA deployments with Split DNS (different domains for inside and outside the network), the HVD must not discover the internal domain. If it does, Cisco Jabber Softphone for VDI registration also fails. To ensure the client does not discover the internal domain, disable UPN during Jabber installation on HVD.

Connection Broker—Installed on the Hosted Virtual Desktops

- Citrix XenApp and XenDesktop 6.x, 7.x (CR—up to 7.18; LTSR—up to 7.15 CU8), and Citrix Virtual Apps and Desktops 7 (CR—up to 2112, LTSR—up to 1912 CU4)
- VMware Horizon versions 6.x to 8.x.

**Important**

Since Citrix Virtual Applications & Desktops 7 2109, "virtual channel allow list policy" is enabled by default. Either configure this policy for JVDI first (by adding Cisco Virtual Channel) for optimized mode to work properly or disable this policy.

```
CISCO,C:\Program Files (x86)\Cisco Systems\Vxc\hvdagent.exe
```

A connection broker is software that creates connections to hosted virtual desktops. A connection broker performs a number of tasks including the following:

- Validating the username and providing a connection for the user.
- Allowing the user to connect to a specific virtual desktop.

Operating Systems—Installed on the Hosted Virtual Desktops

- Microsoft Windows 8.1 32-bit
- Microsoft Windows 8.1 64-bit
- Microsoft Windows 10 32-bit
- Microsoft Windows 10 64-bit
- Microsoft Windows 11 64-bit (as of Jabber VDI 14.0.3)

Server Operating Systems—Installed on the Hosted Virtual Desktops

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Port Requirements

Cisco Jabber Softphone for VDI requires the same ports as Cisco Jabber does, and the following additional port range:

Table 1: Port Usage

Port Range	Description
16384–32767	UDP Inbound and outbound traffic for RTP (audio and video streams) You can configure the Cisco Unified Communications Manager to reduce this port range. Change the Start/Stop Media Port setting in the SIP Profile, which is associated with the CSF device.

Supported Codecs

Supported Codecs

Audio Codecs:

- G.722
- G.722.1 (24 and 32k)
G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.
- G.711 A-law
- G.711 u-law
- G.729a
- Opus
Opus is supported on Cisco Unified Communications Manager 11.0 or later.

Video Codec: H.264/AVC

Requirements—HP Thin Pro

Citrix Workspace app or VMware Horizon Client—Installed on the Thin Clients

The HP Thin Pro image includes the required Citrix and VMware versions.

The Citrix Workspace app or VMware Horizon Client provides a user interface for the corresponding connection broker.

Published application mode and the scale to fit option are not supported.

HP Thin Pro Thin Clients—Hardware

We recommend the following client hardware, which was tested with HP Thin Pro 6.2:

- HP t520
- HP t530
- HP t620
- HP t630
- HP t730
- HP mt21

We recommend the following client hardware, which was tested with HP Thin Pro 7.1 SP3.3:

- HP t430
- HP t520

- HP t530
- HP t630
- HP t730
- HP mt21

HP ThinPro Platform Image

32-bit: HP ThinPro 6.2

64-bit: HP ThinPro 7.1 SP3.3 and 7.x versions



Important Only the components, versions, and minimum hardware requirements listed in this guide are supported. Use of unsupported components can result in a nonfunctional deployment.

Requirements—MacOS

Supported Operating Systems

Cisco Jabber Softphone for VDI 14.0 is supported on the following MacOS versions:

- Mojave (10.14)
- Catalina (10.15)
- Big Sur (11)
- Monterey (12)—As of 14.0.3

Hardware Requirements

Requirement	Cisco Jabber for Mac
Installed RAM	2 GB RAM
Free physical memory	1 GB
Free disk space	300 MB

Requirement	Cisco Jabber for Mac
CPU speed and type	<p>Intel Core 2 Duo or later processors on any of the following Apple hardware:</p> <ul style="list-style-type: none"> • iMac Pro • MacBook Pro • MacBook • MacBook Air • iMac • Mac Mini <p>Cisco Jabber Softphone for VDI also supports Apple M1 processors.</p>
I/O ports	USB 2.0 for USB camera and audio devices

Citrix and VMware Requirements

This release Cisco Jabber Softphone for VDI for Mac OS works in Citrix and VMware VDI environments. You must install the latest Citrix Workspace client (not the Citrix Receiver client) or VMware Horizon client before you install the Cisco JVDI Client.

- Citrix Receiver 13.0 and later
- Citrix Workspace app 1808 and later
- VMware Horizon View Client versions 5.5, 8.0, or 8.1

The Citrix Workspace app or VMware Horizon Client provides a user interface for the corresponding connection broker.

Published application mode and the scale to fit option are not supported.

Requirements—Ubuntu



Important

Only the components, versions, and minimum hardware requirements listed in this guide are supported. Use of unsupported components can result in a nonfunctional deployment.

Ubuntu Desktop Image

- Ubuntu 14.04 32b LTS (i386)
- Ubuntu 16.04 64b LTS (AMD64)
- Ubuntu 18.04 64b LTS (AMD64)
- Ubuntu 20.04 64b LTS (AMD64)



Note The supported versions do not include Ubuntu Minimal.

Ubuntu Thin Clients—Hardware

The minimum hardware requirements for thin clients are as follows:

- Installed RAM 2 GB
- Free Physical Memory 1 GB
- Free Disk Space 256 MB
- CPU: AMD G-T56N 1.65Ghz, or Intel Core2Duo T7500 2.2 GHz
- USB 2.0 for USB camera and audio devices

Citrix Workspace app or VMware Horizon Client—Installed on the Thin Clients

- Citrix Receiver 13.0 and later
- Citrix Workspace app 1808 and later
- VMware Horizon View Client versions 4.x, 5.x, and 8.x

The Citrix Workspace app or VMware Horizon Client provides a user interface for the corresponding connection broker.

Published application mode and the scale to fit option are not supported.

Requirements—Unicon eLux



Important Only the components, versions, and minimum hardware requirements listed in this guide are supported. Use of unsupported components can result in a nonfunctional deployment.

Unicon eLux Platform Image

- 64-bit: Unicon eLux 6.5
- 64-bit: Unicon eLux 6.8
- 64-bit: Unicon eLux 6.9
- 64-bit: Unicon eLux RP6 LTSR 2104 Cu2 (as of Release 14.0.4)

The eLux packages are available from Unicon eLux. For assistance locating a download, contact eLux support.

Unicon eLux Thin Clients—Hardware

The minimum hardware requirements for thin clients are:

- 1.6 GHz dual-core processor
- 2 GB RAM

We recommend the following client hardware, which was tested with eLux RP 5.7.0:

- HP T620 Dual Core / Quad Core
- HP T630 Dual Core / Quad Core
- HP T730
- Cisco VXC 6215
- Dell Wyse Z50D

Citrix Workspace App or VMware Horizon Client—Installed on the Thin Clients

Unicon eLux includes the required Citrix and VMware versions.

The Citrix Workspace app or VMware Horizon Client provides a user interface for the corresponding connection broker.

Published application mode and the scale to fit option are not supported.

Cisco Anyconnect (Optional)

vpnsystem V4.5-1

Requirements—Windows



Important

Only the components, versions, and minimum hardware requirements listed in this guide are supported. Use of unsupported components can result in a nonfunctional deployment.

Microsoft Windows Thin Clients—Hardware

The minimum system requirements for thin clients are as follows:

- Installed RAM 2 GB
- Free Physical Memory 1 GB
- Free Disk Space 256 MB
- CPU Mobile AMD Sempron Processor 3600+, 2-GHz Intel Core 2 CPU, or T7400 2.16 GHz
- DirectX 11 compatible GPU
- USB 2.0 for USB camera and audio devices

Microsoft Windows—Installed on the Thin Clients

- Microsoft Windows 8.1 32-bit

- Microsoft Windows 8.1 64-bit
- Microsoft Windows 10 32-bit
- Microsoft Windows 10 64-bit
- Microsoft Windows 11 64-bit



Note Cisco Jabber Softphone for VDI for Windows does not require the Microsoft .NET Framework or any Java modules.

Windows Embedded Standard Thin Clients—Hardware

The minimum system requirements for thin clients are as follows:

- Installed RAM 2 GB
- Free Physical Memory 1 GB
- Free Disk Space 256 MB
- CPU performance affects the maximum video resolution. With Windows Embedded Standard thin clients, the expected resolution depends on the CPU:
 - Up to 720p with quad-core AMD GX-420CA SOC 2 GHz or similar
 - Up to 240p with dual-core AMD G-T56N 1.65 GHz or similar
 - Audio-only support with dual-core VIA Eden X2 U4200 1 GHz or similar CPU



Note These hardware specifications are only guidelines for the expected resolutions. Other factors can affect video resolution.

- DirectX 11 compatible GPU
- USB 2.0 for USB camera and audio devices

Windows Embedded Standard—Installed on the Thin Clients

- Windows Embedded Standard 8 64-bit
Requires Update for Windows Embedded Standard 8 for 64-bit Systems (KB4019990)
- Windows 10 IoT Enterprise

Citrix Workspace App or VMware Horizon Client—Installed on the Thin Clients

- Citrix Receiver (ICA) for Windows 4.4 and later
- Citrix Workspace App (ICA) for Windows 1808 and later



Important Cisco Jabber Softphone for VDI does not support Citrix Workspace App downloaded from the Microsoft Store.

- VMware Horizon Client for Windows 4.1.0 and later
(Versions 4.3 and 4.4 are not supported.)

The Citrix Workspace app or VMware Horizon Client provides a user interface for the corresponding connection broker.



Important Before you install the Cisco JVDI Client, install the Citrix Receiver or VMware Horizon Client on the thin client.

If you change from a Citrix environment to a VMware environment (or from VMware to Citrix), reinstall the Cisco JVDI Client.

Cisco Jabber Softphone for VDI supports full-screen and windowed display for Windows and Linux thin clients in both VMWare and Citrix VDI environments.



PART I

Deployment

- [Deployment Overview, on page 17](#)
- [Downloads, on page 19](#)
- [Installation, on page 21](#)
- [Configuration, on page 29](#)
- [Upgrade, on page 35](#)



CHAPTER 2

Deployment Overview

- [Deployment Overview Workflow, on page 17](#)

Deployment Overview Workflow

We recommend that you read the release notes document for your platform. Review the requirements to confirm that all hardware and software meet them. Failure to meet all requirements can result in a nonfunctional deployment.

Step 1 Follow the instructions to deploy Cisco Jabber for Windows, up to the installation of the Jabber client.

Important You must create CSF devices for Cisco Jabber Softphone for VDI users, and add each user to the following Access Control Groups:

- Standard CCM End Users
- Standard CTI Enabled
- Standard CTI Allow Call Recording (Required for ad-hoc recording/Built in Bridge functionality)

See *On-Premises Deployment for Cisco Jabber* for your release.

For hybrid deployments, see *Cloud and Hybrid Deployments for Cisco Jabber* for your release.

Cisco Jabber deployment guides are available from: <https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>.

Step 2 Create and set up the hosted virtual desktops in the data center.

Ensure that the hosted virtual desktops (HVD) are ready for you to install the Cisco JVDI Agent. See [Set up the Hosted Virtual Desktops Workflow, on page 21](#).

Step 3 Set up and configure the thin clients.

See the documentation for the thin clients.

Step 4 Install the Cisco Jabber Softphone for VDI components on the thin clients and the HVDs.

- [Install the Components Workflow—HP Thin Pro, on page 22](#)
- [Install the Components Workflow—MacOS, on page 23](#)

- [Install the Components Workflow—Ubuntu, on page 24](#)
- [Install the Components Workflow—Unicon eLux, on page 25](#)
- [Install the Components Workflow—Windows, on page 26](#)

Step 5 Follow the version support strategy, outlined in this guide and in the release notes for your release.



CHAPTER 3

Downloads

- [Download the Cisco JVDI Agent, on page 19](#)
- [Download the Cisco JVDI Client, on page 19](#)
- [Download Cisco AnyConnect—Unicon eLux, on page 20](#)

Download the Cisco JVDI Agent

- Step 1** Visit the following URL:
<https://software.cisco.com/download/>
- Step 2** Click **Browse all**, navigate to **Unified Communications > Unified Communications Applications > Messaging**, and then select your Cisco Jabber Softphone for VDI platform:
- **Cisco Jabber Softphone for VDI—Apple MacOS**
 - **Cisco Jabber Softphone for VDI—Thin Pro and Ubuntu**
 - **Cisco Jabber Softphone for VDI—Unicon eLux**
 - **Cisco Jabber Softphone for VDI—Windows**
- Step 3** From the list, choose the Cisco JVDI Agent file for your release.
- Step 4** Click **Download** or **Add to cart** and follow the prompts.
-

Download the Cisco JVDI Client

This procedure applies to the HP Thin Pro 7.1 SP3, Unicon eLux, and Windows platforms. For HP Thin Pro 6.2, the Cisco Jabber Softphone for VDI Debian (.deb) package and cisco-jvdi<xx.x.x>-pre-reqs.xar file are available from HP. For Ubuntu, the Debian package is available from the Ubuntu Software Center.

- Step 1** Visit the following URL:
<https://software.cisco.com/download/>

- Step 2** Click **Browse all**, navigate to **Unified Communications > Unified Communications Applications > Messaging**, and then select your Cisco Jabber Softphone for VDI platform:
- **Cisco Jabber Softphone for VDI—Apple MacOS**
 - **Cisco Jabber Softphone for VDI—Thin Pro and Ubuntu**
 - **Cisco Jabber Softphone for VDI—Unicon eLux**
 - **Cisco Jabber Softphone for VDI—Windows**
- Step 3** From the list, choose the Cisco JVDI Client file for your release.
- Step 4** Click **Download** or **Add to cart** and follow the prompts.
-

Download Cisco AnyConnect—Unicon eLux

The supported **vpnsystem** package is available from Unicon.

- Step 1** Visit the Unicon web site.
- Step 2** Locate and download the file: **vpnsystem**.
- For assistance locating the file, contact Unicon support.
-



CHAPTER 4

Installation

- [Set up the Hosted Virtual Desktops Workflow, on page 21](#)
- [Install the Components Workflow—HP Thin Pro, on page 22](#)
- [Install the Components Workflow—MacOS, on page 23](#)
- [Install the Components Workflow—Ubuntu, on page 24](#)
- [Install the Components Workflow—Unicon eLux, on page 25](#)
- [Install the Components Workflow—Windows, on page 26](#)

Set up the Hosted Virtual Desktops Workflow

The Virtual Machines for the HVDs can be either Citrix-, or VMware-provisioned. Citrix-provisioned virtual machines can be dedicated, or have multiple users connected over multiple remote sessions. To support multiple remote sessions, the virtual machine must be running a supported Microsoft Windows Server operating system.

-
- Step 1** Log in to the Microsoft Windows HVD as the new user, with administration rights.
- Step 2** Join the HVD to the corporate domain.
You must have domain administration rights.
- Step 3** Set up Citrix or VMware access to the HVDs.
-

What to do next

- [Install the Components Workflow—HP Thin Pro, on page 22](#)
- [Install the Components Workflow—MacOS, on page 23](#)
- [Install the Components Workflow—Ubuntu, on page 24](#)
- [Install the Components Workflow—Unicon eLux, on page 25](#)
- [Install the Components Workflow—Windows, on page 26](#)

Install the Components Workflow—HP Thin Pro

Before you begin

Ensure that you have all of the required files on hand. If you plan to manually install Cisco JVDI Client on the thin clients, copy the files to a USB stick.

- Follow the guidelines in the [Version Support Strategy](#), on page 35.
- [Download the Cisco JVDI Agent](#), on page 19
- [Download the Cisco JVDI Client](#), on page 19



Note Starting with Thin Pro 7.1 SP3, the prerequisites file is pre-installed with Thin Pro. For Thin Pro 6.2, you can obtain the prerequisites file directly from HP.

Step 1 On the thin client, install the Cisco Jabber Softphone for VDI files in the following order, either manually from a USB stick, or use HP Device Manager for mass deployments.

Order of installation:

- a. Prerequisites
- b. Cisco Jabber Softphone for VDI .deb package.

For more information about mass deployment, see the documentation for HP Device Manager 4.7, available from HP.

Step 2 On the HVD, install Cisco JVDI Agent.

Double-click the .msi file, and then follow the installation wizard steps.

Step 3 On the HVD, install Cisco Jabber for Windows.

Double-click CiscoJabberSetup.msi and follow the installation wizard steps. For detailed information about how to install Cisco Jabber for Windows, see *On-Premises Deployment for Cisco Jabber* for your release.

For hybrid deployments, see *Cloud and Hybrid Deployments for Cisco Jabber* for your release.

Cisco Jabber deployment guides are available from: <https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>.

What to do next

Clone the HVD. For best practices for cloning Microsoft Windows HVD images, consult the documentation for your Citrix or VMware product.

Create an image for the thin clients. See the documentation for HP Device Manager 4.7, available from HP.

Install the Components Workflow—MacOS

Before you begin

- Follow the guidelines in the [Version Support Strategy, on page 35](#).
- [Download the Cisco JVDI Agent, on page 19](#)
- [Download the Cisco JVDI Client, on page 19](#)

Procedure

	Command or Action	Purpose
Step 1	On the HVD, install Cisco JVDI Agent.	
Step 2	On the HVD, install Cisco Jabber.	<p>Double-click CiscoJabberSetup.msi and follow the installation wizard steps. For detailed information about how to install Cisco Jabber for Windows, see <i>On-Premises Deployment for Cisco Jabber</i> for your release.</p> <p>For hybrid deployments, see <i>Cloud and Hybrid Deployments for Cisco Jabber</i> for your release.</p> <p>Cisco Jabber deployment guides are available from: https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.</p>
Step 3	On the thin client, install the Cisco JVDI Client.	See Run the MacOS Installer, on page 23 .

Run the MacOS Installer

Run the MacOS installer (PKG) to install Cisco JVDI Client.

-
- Step 1** Double-click the Install_Cisco_JVDI_Client.pkg file.
- Step 2** Read the EULA and, if you agree, click **Continue**.
- Step 3** Click **Install**, and if a prompt appears that Citrix Viewer must be closed first, click **Close Application and Install**.
You can also click **Install Later** if you cannot close Citrix at the time.
- Step 4** Click through the remaining screens to complete the installation.
-

Accept permissions

When users launch the Cisco JVDI Client on Mac OS for the first time, accept the following required permissions:

Table 2: Required permissions

Permission	Description
Access Camera	Uses the camera in a video call, or trying to open the camera in Settings.
Access Microphone	Uses the microphone for voice in a call.
Record Screen	Uses the camera in a video call, or trying to open the camera in Settings.
Access Accessibility	Required for matching the Cisco JVDI Client to the Citrix viewer. After maximizing the application on Mac OS, the application window is put into a new virtual desktop (or space). If users maximize the Citrix viewer, Jabber's video overlay window joins the space of the Citrix viewer. To do this, JVDI need request to access the system's Accessibility. User would see this pop-up in the first time of running JVDI.

Install the Components Workflow—Ubuntu

Before you begin

Ensure that you have all of the required files on hand. If you plan to manually install Cisco JVDI Client on the thin clients, copy the files to a USB stick.

- Follow the guidelines in the [Version Support Strategy](#), on page 35.
- [Download the Cisco JVDI Agent](#), on page 19
- Obtain the Cisco Jabber Softphone for VDI deb package from the Ubuntu software center repository.

On the thin client, use the terminal emulator to run the following command: **sudo apt-get update**, and then enter your password at the prompt. The list of repositories for the Ubuntu Software Center updates. After the command finishes reading the package lists, you can close the terminal emulator. You can place the file on a network share accessible from the thin clients, or copy it to a USB stick.

Step 1 On the HVD, install Cisco JVDI Agent.

Double-click the Cisco JVDI Agent .msi and follow the installation wizard steps.

Step 2 On the HVD, install Cisco Jabber; double-click CiscoJabberSetup.msi and follow the installation wizard steps.

For detailed information about how to install Cisco Jabber for Windows, see *On-Premises Deployment for Cisco Jabber* for your release.

For hybrid deployments, see *Cloud and Hybrid Deployments for Cisco Jabber* for your release.

Cisco Jabber deployment guides are available from: <https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>.

Step 3 On the thin client, install the Cisco JVDI Client; enter your password at the authentication prompt.

When you double-click the Cisco Jabber Softphone for VDI deb package, the Ubuntu Software Center opens. After you click **Install**, the Ubuntu Software Center locates and installs the dependency libraries, and then installs the Cisco JVDI Client.

What to do next

Clone the HVD image. For best practices for cloning Microsoft Windows HVD images, consult the documentation for your Citrix or VMware product.

Create an image for the thin clients.

Install the Components Workflow—Unicon eLux

Before you begin

- Follow the guidelines in the [Version Support Strategy, on page 35](#).
- [Download the Cisco JVDI Agent, on page 19](#)
- [Download the Cisco JVDI Client, on page 19](#)
- [Download Cisco AnyConnect—Unicon eLux, on page 20](#) (Optional, required only if users need VPN connectivity.)

Step 1 On the HVD, install Cisco Jabber for Windows.

Double-click CiscoJabberSetup.msi and follow the installation wizard steps. For detailed information about how to install Cisco Jabber for Windows, see *On-Premises Deployment for Cisco Jabber* for your release.

For hybrid deployments, see *Cloud and Hybrid Deployments for Cisco Jabber* for your release.

Cisco Jabber deployment guides are available from: <https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>.

Step 2 On the HVD, install Cisco JVDI Agent.

Double-click the MSI file and follow the installation wizard steps.

Step 3 On the thin client, install the Cisco JVDI Client and if required, deploy Cisco AnyConnect at the same time.

What to do next

Clone the HVD image. For best practices for cloning Microsoft Windows HVD images, consult the documentation for your Citrix or VMware product.

Use the Elias tool to create an image that contains Cisco JVDI Client. Deploy the image to the thin clients. For more information about how to create an image or how to update the thin client, see the Elias documentation available from the Unicon website.

Install the Components Workflow—Windows

Before you begin

- Follow the guidelines in the [Version Support Strategy](#), on page 35.
- [Download the Cisco JVDI Agent](#), on page 19
- [Download the Cisco JVDI Client](#), on page 19

Step 1 On the HVD, install Cisco JVDI Agent.

Step 2 On the HVD, install Cisco Jabber.

Double-click CiscoJabberSetup.msi and follow the installation wizard steps. For detailed information about how to install Cisco Jabber for Windows, see *On-Premises Deployment for Cisco Jabber* for your release.

For hybrid deployments, see *Cloud and Hybrid Deployments for Cisco Jabber* for your release.

Cisco Jabber deployment guides are available from: <https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>.

Step 3 On the thin client, install the Cisco JVDI Client.

See [Cisco JVDI Client Installation](#), on page 26.

Cisco JVDI Client Installation

Prerequisites

Before you install Cisco JVDI Client on the thin clients, complete the following tasks:

- Install and set up the Citrix Receiver or VMware Horizon View Client.



Note The JVDI Client is available as a 32- or 64-bit application.

- Obtain the Cisco JVDI Client zip file, and extract the contents.

Use one of the following methods to install Cisco JVDI Client:

- [Run the Microsoft Installer](#), on page 27
- [Use the Command Line](#), on page 27
- [Use the Group Policy Editor](#), on page 27

Run the Microsoft Installer

Run the Microsoft Installer (MSI) to install Cisco JVDI Client.

-
- Step 1** Double-click the CiscoJVDIClientSetup.msi file.
- Step 2** To open the executable file, click **OK**.
- Step 3** If the **Open File - Security Warning** appears, click **Run**.
- Step 4** Read the EULA and, if you agree, click **Accept and Install**.
<http://www.cisco.com/go/eula>.
- Step 5** To complete the installation, click **Finish**.
-

Use the Command Line

-
- Step 1** Open a command window.
- Step 2** Enter the following command: `start /wait msiexec.exe /i <path to MSI>\CiscoJVDIClientSetup.msi /quiet`.
The `/quiet` switch specifies a silent installation.
-

Use the Group Policy Editor

Use the Group Policy Management console to deploy Cisco JVDI Client to supported thin clients that are running a supported Microsoft Windows operating system.

Before you begin

- Use Microsoft Orca to set the language code to 1033.
 - Copy the modified Microsoft Installer (MSI) to a software distribution point for deployment. All computers to which you plan to deploy Cisco JVDI Client must be able to access the MSI on the distribution point.
-

- Step 1** Select **Start > Run**.
- Step 2** At the prompt, enter the following command: `GPMC.msc`.
- Step 3** Right-click on the appropriate domain in the left section.
- Step 4** Select **Create a GPO in this Domain, and Link it here**.
- Step 5** In the **New GPO** window, **Name** field, enter a name for the group policy object.
- Step 6** Leave the default value or select an option from the **Source Starter GPO** list, and then select **OK**.
The new group policy appears in the list of group policies for the domain.
- Step 7** Select the group policy object under the domain in the left section.

- Step 8** From the **Security Filtering** section of the **Scope** tab, select **Add**.
- Step 9** Specify the computers and users to which you want to deploy Cisco JVDI Client.
- Step 10** Specify the MSI file.
- Step 11** Right-click the group policy object in the left section and then select **Edit**.
The Group Policy Management Editor opens.
- Step 12** Select **Computer Configuration** and then select **Policies > Software Settings**.
- Step 13** Right-click **Software Installation** and then select **New > Package**.
- Step 14** Next to **File Name**, enter the location of the MSI file.

Example:

```
\\server\software_distribution
```

Important Enter the Uniform Naming Convention (UNC) path for the location of the MSI file. If you do not enter the UNC path, Group Policy cannot deploy Cisco JVDI Client.

- Step 15** Select the MSI file, and then select **Open**.
- Step 16** In the **Deploy Software** dialog box, select **Assigned**, and then select **OK**.
-



CHAPTER 5

Configuration

- [Configuration Files, on page 29](#)
- [Set up Users on the Cisco Unified Communications Manager Workflow, on page 29](#)
- [Change a User Password, on page 33](#)

Configuration Files

For each Cisco Unified Client Services Framework (CSF) device that you add to the system, Cisco Unified Communications Manager creates a configuration (CNF.xml) file. The CNF file contains the device specifications for the associated user.

When users sign in to Cisco Jabber, Cisco Jabber Softphone for VDI starts the download of the associated CNF file to the thin client. To ensure the successful transfer of the file, open the relevant ports in all firewall applications to allow the thin client to access the ports. For more information about how to open ports, see the documentation for the firewall software.



Important

Download of the CNF.xml file follows the system setting for HTTP proxy. Ensure that the proxy does not route the HTTP request from the thin client outside of the corporate network.

Set up Users on the Cisco Unified Communications Manager Workflow

- Step 1** [Create a CSF Device and a Directory Number for Each User, on page 30.](#)
- Step 2** [Associate New Devices with a User, on page 32.](#)
- Step 3** [Enable the CTI Protocol for Users, on page 32.](#)
- Step 4** [Configure Cisco Unified Communications Features for Users, on page 33.](#)

Enable the Unified Communications Manager IM and Presence Service. See the documentation for your version of Cisco Unified Communications Manager.

Create a CSF Device and a Directory Number for Each User

You can use the same Cisco Unified Client Services Framework (CSF) devices for the virtual environment, as you do for the nonvirtual environment. We recommend that you create only one CSF device for each virtual user. If multiple devices exist for a virtual user, virtual Jabber automatically selects the first device in the list.

Step 1 From Cisco Unified Communications Manager Administration, choose **Device > Phone**.

Step 2 Select **Add New**.

Step 3 From the **Phone Type** drop-down list, choose **Cisco Unified Client Services Framework**, and then select **Next**.

Step 4 In the **Phone Configuration** window, enter the applicable information for the phone as follows:

Option	Description
Device Name	Enter a name to identify the Cisco Unified Client Services Framework device. The name can contain 1 to 15 characters, including alphanumeric characters. Periods, hyphens, and underscores are not supported. Typically the device name format is CSF<username>; however, including the user ID is optional. Example: CSFjohndoe.
Description	Enter a descriptive name for the phone. For example, enter <i>Richard-phone-on-computer</i> .
Device Pool	Choose Default or another profile that was previously created. The device pool defines sets of common characteristics for devices. These characteristics include the region, the date and time group, the softkey template, and Multilevel Precedence and Preemption (MLPP) information.
Phone Button Template	Choose Standard Client Services Framework . The phone button template determines the configuration of buttons on a phone and identifies which feature (such as line or speed dial) is used for each button. This option is required.
Owner User ID	To use an adjunct license with this device, choose the user ID from the list.
Primary Phone	To use an adjunct license with this device, choose the device name of the Cisco Unified IP Phone to associate with the client application.
Allow Control of Device from CTI	Always check this option in a virtual environment.
Presence Group	Choose Standard Presence Group .
Device Security Profile	Choose Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile .
SIP Profile	Choose Standard SIP Profile or another profile that was previously created. SIP profiles provide specific SIP information for the phone, such as registration and keepalive timers, media ports, and Do Not Disturb control.

Option	Description
	Important If you choose Secure Phone Profile , do not specify the Certificate Authority Proxy Function (CAPF) authentication mode By Null string . Use of this setting with Cisco Jabber Softphone for VDI causes Jabber registration with Cisco Unified Communications Manager to fail.

Step 5 Scroll down to the **Product Specific Configuration Layout** section, and set **Video Calling** to **Enabled**.

Step 6 Select **Save**.

Step 7 Select **Apply Config** if this button is available, and then confirm when prompted.

Step 8 Select **Add a new DN** in the **Association Information** section that appears on the left side of the window.

Step 9 Enter information for the directory number on the **Directory Number Configuration** window.

Option	Description
Directory Number	Enter the directory number (line) to assign to the device.
Route Partition	Enter the route partition. Partitions divide the route plan into logical subsets. These subsets include organization, location, and type of call.
Display (Internal Caller ID)	Enter the Caller ID. This entry is optional. The actual display depends on this entry and the configuration for the other party. For example, Cisco IP Phones display the Caller ID, but Cisco Jabber does not.
Maximum Number of Calls	Specify the maximum number of calls that can be presented to the application. This number includes all calls placed on hold plus the active call, regardless of which party initiated the calls.
Busy Trigger	Specify the number of calls (active and on hold). Incoming calls, above this limit receive a busy signal or are redirected to the Forward Busy Internal/External target (if the target is configured).

Step 10 Select **Save**.

Step 11 Select **Apply Config** if this button is available, and then confirm when prompted.

Step 12 Scroll to the bottom of the **Directory Number Configuration** window, and then select **Associate End Users**.

Step 13 In the **Find and List Users** window, use the search criteria to find the user who you want to associate with the directory number.

Step 14 Check the box next to that username, and then select **Add Selected**.

The user is now associated with the DN.

Step 15 In the **User Associated with Line** section of the window, select the username.

Step 16 In the **End User Configuration** window, scroll down to the **Direct Number Associations** section.

Step 17 From the **Primary Extension** drop-down list, choose the DN for the user.

Step 18 In the **End User Configuration** window, under **Permissions Information**, select **Add to User Group** or **Add to Access Control Group**, depending on your version of Cisco Unified Communications Manager.

Step 19 In the **Find and List User Groups** window, use the search criteria to find **Standard CCM End Users**.

Step 20 Check the box next to **Standard CCM End Users**, and then select **Add Selected**.

Step 21 In the **Find and List User Groups** window, use the search criteria to find **Standard CTI Enabled**.

Step 22 Check the box next to **Standard CTI Enabled**, and then select **Add Selected**.

Step 23 Select **Save**.

Cisco Unified Communications Manager reminds you that changes to line or directory number settings require a restart. However, you need only restart after you edit lines on Cisco Unified IP Phones that are running at the time of the modifications.

Associate New Devices with a User



Note Perform this task in Cisco Unified Communications Manager.

Step 1 From Cisco Unified Communications Manager Administration, choose **> User Management > End User**.

Step 2 Search for the user in the **Find and List Users** window.

Step 3 Select the user.

Step 4 Select **Device Association** in the **Device Information** section.

Step 5 Search for the devices that you require in the **User Device Association** window.

Step 6 Select the devices that you require.

For example, you can select a device whose type is Cisco Unified Client Services Framework, and a desk-phone device.

Step 7 Select **Save Selected/Changes**.

Step 8 Select **Back to User** from the menu in the **Related Links** navigation box at the top right of the window.

Step 9 Select **Go**.

Step 10 Verify that the devices are listed in the **Device Information** section in the **End User Configuration** window.

Enable the CTI Protocol for Users

Enable the computer-telephony integration (CTI) protocol for each Cisco Jabber Softphone for VDI user.

Step 1 In Cisco Unified Communications Manager Administration, click **User Management > End Users**.

Step 2 Search for the user in the **Find and List Users** window.

Step 3 Select the user.

Step 4 In the **End User Configuration** window, scroll down to Permissions Information.

Step 5 Click **Add to User Group**.

Step 6 Select the following required groups:

- Standard CCM End Users
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

Step 7 Select the following groups if want to configure selective call recording:

- Standard CTI Allow Call Recording
- Standard CTI Allow Call Monitoring

Step 8 Click **Save**.

What to do next

Enable the Unified Communications Manager IM and Presence Service. See the documentation for your version of Cisco Unified Communications Manager.

Configure Cisco Unified Communications Features for Users

For information about how to configure Cisco Unified Communications features for Cisco Jabber, see the deployment and installation guide for your release, available from <http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>.

Change a User Password

Use this procedure to change the password for a user only if LDAP Authentication is not enabled. If LDAP Authentication is enabled, the passwords are stored on the LDAP Server. For Cisco Unified Communications Manager 9.0 or later, this procedure applies only to passwords for users created locally.

SUMMARY STEPS

1. From Cisco Unified Communications Manager Administration, choose **Cisco Unified Communications Manager Administration > User Management > End User**.
2. Search for the user in the **Find and List Users** window.
3. Select the user.
4. In the **End User Configuration** window, in the **Password** field, enter a new password for the user.
5. In the **Confirm Password** field, enter the new password for the user again.
6. Select **Save**.

DETAILED STEPS

- Step 1** From Cisco Unified Communications Manager Administration, choose **Cisco Unified Communications Manager Administration > User Management > End User**.
- Step 2** Search for the user in the **Find and List Users** window.
- Step 3** Select the user.
- Step 4** In the **End User Configuration** window, in the **Password** field, enter a new password for the user.
- Step 5** In the **Confirm Password** field, enter the new password for the user again.

Step 6 Select **Save**.



CHAPTER 6

Upgrade

- [Upgrade Notes, on page 35](#)
- [Version Support Strategy, on page 35](#)
- [Upgrade Workflow, on page 36](#)

Upgrade Notes

To get the new Cisco Jabber Softphone for VDI features, you must upgrade all of the following components to the current release:

- Cisco Jabber for Windows
- Cisco JVDI Agent
- Cisco JVDI Client

Both the Cisco JVDI Agent and Cisco JVDI Client are required for softphone registration to succeed. The Cisco Jabber for Windows and the Cisco JVDI Agent versions must always match. However, the Cisco JVDI Client version can be the same, or up to two releases earlier. The earlier software version determines the available feature set.

Version Support Strategy

- The Cisco Jabber for Windows and Cisco JVDI Agent major versions (N.A) must always match. However, the JVDI Client version can be the same, or up to two releases earlier (N-2 support).



Note N.A-C denotes the range of major releases. x-z denotes the numbers of different maintenance releases. These numbers are used for example purposes only.

For example, the following version combinations are supported within a release range:

- Cisco Jabber for Windows Release N.A(x), Cisco JVDI Agent Release N.A(y), and Cisco JVDI Client Release N.A(z)

- Cisco Jabber for Windows Release N.A(x), Cisco JVDI Agent Release N.A(y), and Cisco JVDI Client Release N.B(z)
- Cisco Jabber for Windows Release N.A(x), Cisco JVDI Agent Release N.A(y), and Cisco JVDI Client Release N.C(z)



Note The above examples cover the supported range within a single major release. For a major release that starts at a new release number (for example, 14.0), the JVDI client is also supported on the two previous releases (for example, 12.9 and 12.8).

The following version combinations are not supported within a release range:

- Cisco Jabber for Windows Release N.A(x), Cisco JVDI Agent Release N.A(y), and Cisco JVDI Client Release N.D(z)
- Cisco Jabber for Windows Release N.A(x), Cisco JVDI Agent Release N.B(y), and Cisco JVDI Client Release N.C(z)

Upgrade Workflow

We recommend that you read the release notes document for your platform. Review the requirements to confirm that all hardware and software meet them. Failure to meet all requirements can result in a nonfunctional deployment.

Before you begin

Ensure that you have all of the required files on hand. If you plan to manually install Cisco JVDI Client on the thin clients, copy the files to a USB stick.

Follow the steps to install the Cisco Jabber Softphone for VDI components on the thin clients and the HVDs.

- [Install the Components Workflow—HP Thin Pro, on page 22](#)
- [Install the Components Workflow—MacOS, on page 23](#)
- [Install the Components Workflow—Ubuntu, on page 24](#)
- [Install the Components Workflow—Unicon eLux, on page 25](#)
- [Install the Components Workflow—Windows, on page 26](#)

Important Both the Cisco JVDI Agent and Cisco JVDI Client are required for softphone registration to succeed. The Cisco Jabber for Windows and Cisco JVDI Agent versions must always match. However, the Cisco JVDI Client version can be the same, or the previous version. The earlier software version determines the available feature set.

If you're not upgrading the Cisco JVDI Client, you can skip the steps to install it.



PART II

Troubleshooting

- [General Troubleshooting, on page 41](#)
- [Troubleshooting—HP Thin Pro and Ubuntu, on page 45](#)
- [Troubleshooting—Unicon eLux, on page 49](#)
- [Troubleshooting—Windows, on page 51](#)



CHAPTER 7

General Troubleshooting

- [Problem Reporting Tool](#), on page 41
- [Virtual Channel Problem](#), on page 42
- [Configuration Files](#), on page 42
- [Verify That Cisco JVDI Agent Is Installed](#), on page 42
- [Verify Device Registration with Cisco Unified Communications Manager](#), on page 43
- [Verify the Connection Status in Cisco Jabber](#), on page 43
- [Jabber VDI Fallback Mode](#), on page 43
- [Disable BFCP desktop share](#), on page 44

Problem Reporting Tool

The Problem Reporting Tool (PRT) is a small program that automatically runs if Cisco Jabber encounters an unrecoverable error, unhandled exception, or crash. The tool collects logs from the thin client and hosted virtual desktop and then creates a problem report. The report is a zip file that you can send to the Cisco Technical Assistance Center (TAC), to provide the necessary information to solve the problem. The tool saves the file to the user's desktop. Users must accept the privacy agreement to run the PRT.



Tip Advise users to include a memory dump with the problem report if Cisco Jabber crashes. We also recommend that users provide a description of the circumstances that lead up to the error.

If a user experiences an error that does not crash the software, the user can run the PRT from the Cisco Jabber menu: **Help > Report a problem**.

If Cisco Jabber is not running, users can generate a problem report from the Windows **Start** menu. To access the tool from outside the application, choose **Start > All Programs > Cisco Jabber > Cisco Jabber Problem Report**.



Important Problem reports include logs from the thin client, the hosted virtual desktop, and any detailed information that users enter. You can use this information to help troubleshoot the issue.

If there is a problem with the virtual channel, or if Cisco Jabber is not running, the problem report does not include logs from the thin client. For more information, see [Virtual Channel Problem](#), on page 42.

Virtual Channel Problem

If a problem exists with the virtual channel, the problem-reporting tool cannot collect the logs from the thin client. A problem with the virtual channel can cause the Device Selector to not start or to not populate with devices.

Cisco Technical Assistance Center (TAC) personnel may ask you to gather the logs manually by running one of the following executables:

- **Windows OS 32-bit:** `C:\Program Files (x86)\Cisco Systems\Cisco JVDI\CollectCiscoJVDIClientLogs.exe`
- **Windows OS 64-bit:** `C:\Program Files\Cisco Systems\Cisco JVDI\CollectCiscoJVDIClientLogs.exe`
- **Linux-based OS:** `/usr/bin/collect-files`

The executable gathers the logs from the thin client and saves them to the desktop as a `CiscoJVDIClient-logs[timestamp].7z` file. You can still use the PRT to gather the logs from the hosted virtual desktop. Submit all logs gathered to TAC.

Configuration Files

For each Cisco Unified Client Services Framework (CSF) device that you add to the system, Cisco Unified Communications Manager creates a configuration (CNF.xml) file. The CNF file contains the device specifications for the associated user.

When users sign in to Cisco Jabber, Cisco Jabber Softphone for VDI starts the download of the associated CNF file to the thin client. To ensure the successful transfer of the file, open the relevant ports in all firewall applications to allow the thin client to access the ports. For more information about how to open ports, see the documentation for the firewall software.



Important Download of the CNF.xml file follows the system setting for HTTP proxy. Ensure that the proxy does not route the HTTP request from the thin client outside of the corporate network.

Verify That Cisco JVDI Agent Is Installed

You can use the Windows Control Panel to verify that Cisco JVDI Agent is installed. You can also verify the version.


-
- Step 1** From Control Panel, open **Programs and Features** (Windows 7) or **Programs** (Windows 8 and later).
- Step 2** Scroll through the list of installed programs to locate Cisco JVDI Agent.
- The Cisco JVDI Agent version appears in the **Versions** column.
-

Verify Device Registration with Cisco Unified Communications Manager

After device registration, verify that the CSF device registered to the Cisco Unified Communications Manager from the thin client IP address. For more information, see the documentation for your version of Cisco Unified Communications Manager.

Verify the Connection Status in Cisco Jabber

After you sign in to Cisco Jabber for Windows, you can check the connection status for Jabber and for Cisco Softphone for VDI. You can also confirm the versions for the JVDI Agent and the JVDI Client.

Step 1 Click  to open the **Settings Menu**.

Step 2 Go to **Help > Show connection status**

Step 3 In the **Connection Status** window, click **JVDI Details**.

You can see the following information:

- **JVDI Client version**

Tip If the JVDI Client version is 12.5 or 12.1, the client version doesn't appear until after the softphone connects.

- **JVDI Agent version**

- **Virtual Channel status** indicates whether communication between the JVDI Client and Cisco Jabber is successful.

- **SIP status** indicates whether SIP communication with Cisco Unified Communications Manager is successful.

- **Softphone CTI status** indicates whether CTI communication is successful.

Tip If the **SIP status** is **Connected**, but the **Softphone CTI status** is **Not connected**, check the CTI configuration in CUCM.

Step 4 To see detailed diagnostic information for Cisco Jabber, press **Ctrl +Shift +D**.

Jabber VDI Fallback Mode

Jabber VDI fallback mode offers short-term support for basic audio and video calls when VDI can't establish the virtual channel. Fallback mode supports standard calls and call recording. The full feature set isn't supported. For example, you can't forward a call that you're recording in fallback mode. Call quality is lower because of the server or network issues that cause the switch to fallback mode.

Disable BFCP desktop share

The Jabber parameter `EnableBFCPVideoDesktopShare` might not work properly in JVDI environments.

In Jabber Softphone for VDI Release 14.0.3, we added a JVDI configuration parameter to force the proper behavior if necessary.

ENABLE_BFCP_DESKTOP_SHARE—Applies to JVDI Client for Windows and Linux

Added to fix [CSCwa33411](#). This parameter helps disable BFCP screen sharing if necessary.

You configure this parameter in the `cisco.conf` of JVDI Client. On Windows, `cisco.conf` is in `C:\Program Files\Cisco Systems\Cisco VXME` or `C:\Program Files (x86)\Cisco Systems\Cisco VXME`. On Linux, `cisco.conf` is in `/etc/`

- `true` (default)—Enables BFCP screen sharing
- `false`—Disables BFCP screen sharing



CHAPTER 8

Troubleshooting—HP Thin Pro and Ubuntu

- [Verify the Platform Version—HP Thin Pro, on page 45](#)
- [Verify the Platform Version—Ubuntu, on page 45](#)
- [Verify That the Cisco JVDI Client Is Installed, on page 46](#)
- [Verify That VXC Is Running on the Thin Client, on page 46](#)
- [Call Control Is Lost After a Network Failure, on page 46](#)
- [Call Is Lost After HVD Disconnection, on page 47](#)

Verify the Platform Version—HP Thin Pro

- Step 1** On the thin client, open the terminal console.
- Step 2** Enter the following command: `lsb_release -a`.
- Step 3** Look in the output for the HP Thin Pro version.

Example:

```
HP Thin Pro 5.2
```

Verify the Platform Version—Ubuntu

- Step 1** On the thin client, open **System Settings**.
- Step 2** Select **Details**.
- The version appears under the Ubuntu logo.

Example:

```
Ubuntu 14.04.x 32b LTS
```

Verify That the Cisco JVDI Client Is Installed

Use this procedure to verify that Cisco JVDI Client is installed, and to confirm the version.

- Step 1** On the thin client, open the terminal console.
- Step 2** Enter the following command: `dpkg -l | grep jvdi`.
- Step 3** In the output, look for `ii cisco-jvdi-client`.

Example:

```
ii cisco-jvdi-client <xx.x.x.xxx> i386 Cisco JVDI Client
```

Verify That VXC Is Running on the Thin Client

Cisco Jabber Softphone for VDI requires that the `vxc` process be running.

- Step 1** Use Secure Shell (SSH) to connect to the thin client.
- Step 2** Search the running programs for `vxc`.

`ps -ef | grep -r vxc`

You should see the following lines:

```
admin@LWT44d3ca76ba19:~> ps -ef |grep -r vxc

thinuser 6536 1 0 Mar14 ? 00:07:43 /bin/bash /usr/bin/pidrun.sh -c run_vxc.sh -a -m -o
/var/log/cisco/vxcConsole.log -e /var/log/cisco/vxcError.log

thinuser 6538 6536 0 Mar14 ? 00:00:00 /bin/bash /usr/bin/run_vxc.sh -m

thinuser 6547 6538 8 Mar14 ? 13:02:16 vxc -m

admin 31576 31303 0 11:05 pts/0 00:00:00 grep -r vxc

admin@LWT44d3ca76ba19:~>
```

Call Control Is Lost After a Network Failure

Users see a prompt to reconnect to their hosted virtual desktops (HVDs). After the users reconnect, Cisco Jabber call control features do not work.

This problem can occur if the thin client loses network connectivity.

To resolve this issue, have the users exit Cisco Jabber and disconnect from their HVDs. Next they can log back in to their HVDs and sign back in to Cisco Jabber to restore call control.

Call Is Lost After HVD Disconnection

Users receive a prompt to log back in to their hosted virtual desktops (HVD) during an active call, and the call drops. The other party to the call has no indication that the call has ended, except the line is silent.

This issue can occur if the connection between the thin client and the HVD drops, causing a temporary loss of registration and call control.

To work around this issue, users can call the other party back. If the other party is not available, users can send an instant message (IM).



CHAPTER 9

Troubleshooting—Unicon eLux

- [Verify the Platform Base Image Version, on page 49](#)
- [Verify That Cisco JVDI Client Is Installed, on page 49](#)
- [Verify That VXC Is Running on the Thin Client, on page 49](#)
- [Call Control Is Lost After a Network Failure, on page 50](#)
- [Call Is Lost After HVD Disconnection, on page 50](#)

Verify the Platform Base Image Version

- Step 1** On the **Start** menu, select **Control Panel**.
 - Step 2** Select the **Setup** tab.
 - Step 3** Select the **General** tab and look for the OS line.
-

Verify That Cisco JVDI Client Is Installed

Use this procedure to verify that Cisco JVDI Client is installed, and to confirm the Cisco JVDI Client version.

- Step 1** On the **Start** menu, select **Control Panel**.
 - Step 2** Select the **Setup** tab.
 - Step 3** Select the **General** tab.
 - Step 4** Scroll down the list of packages and look for **Cisco JVDI Client**.
The add-on versions appear in the same line.
-

Verify That VXC Is Running on the Thin Client

Cisco Jabber Softphone for VDI requires that the `vxc` process be running.

Step 1 Use Secure Shell (SSH) to connect to the thin client.

Step 2 Search the running programs for `vxc`.

ps -ef | grep -r vxc

You should see the following lines:

```
admin@LWT44d3ca76ba19:~> ps -ef |grep -r vxc

thinuser 6536 1 0 Mar14 ? 00:07:43 /bin/bash /usr/bin/pidrun.sh -c run_vxc.sh -a -m -o
/var/log/cisco/vxcConsole.log -e /var/log/cisco/vxcError.log

thinuser 6538 6536 0 Mar14 ? 00:00:00 /bin/bash /usr/bin/run_vxc.sh -m

thinuser 6547 6538 8 Mar14 ? 13:02:16 vxc -m

admin 31576 31303 0 11:05 pts/0 00:00:00 grep -r vxc

admin@LWT44d3ca76ba19:~>
```

Call Control Is Lost After a Network Failure

Users see a prompt to reconnect to their hosted virtual desktops (HVDs). After the users reconnect, Cisco Jabber call control features do not work.

This problem can occur if the thin client loses network connectivity.

To resolve this issue, have the users exit Cisco Jabber and disconnect from their HVDs. Next they can log back in to their HVDs and sign back in to Cisco Jabber to restore call control.

Call Is Lost After HVD Disconnection

Users receive a prompt to log back in to their hosted virtual desktops (HVD) during an active call, and the call drops. The other party to the call has no indication that the call has ended, except the line is silent.

This issue can occur if the connection between the thin client and the HVD drops, causing a temporary loss of registration and call control.

To work around this issue, users can call the other party back. If the other party is not available, users can send an instant message (IM).



CHAPTER 10

Troubleshooting—Windows

- [Configuration Files, on page 51](#)
- [Registry Keys, on page 51](#)
- [Verify That Cisco JVDI Client Is Running, on page 52](#)
- [Confirm the Version of Cisco JVDI Client, on page 52](#)
- [Call Control Is Lost After a Network Failure, on page 52](#)
- [Call Is Lost After HVD Disconnection, on page 53](#)
- [Enable Log Collection, on page 53](#)
- [Enable Memory Dump Collection, on page 53](#)
- [Display issues, on page 54](#)

Configuration Files

For each Cisco Unified Client Services Framework (CSF) device that you add to the system, Cisco Unified Communications Manager creates a configuration (CNF.xml) file. The CNF file contains the device specifications for the associated user.

When users sign in to Cisco Jabber, Cisco Jabber Softphone for VDI starts the download of the associated CNF file to the thin client. To ensure the successful transfer of the file, open the relevant ports in all firewall applications to allow the thin client to access the ports. For more information about how to open ports, see the documentation for the firewall software.



Important

Download of the CNF.xml file follows the system setting for HTTP proxy. Ensure that the proxy does not route the HTTP request from the thin client outside of the corporate network.

Registry Keys

The Cisco JVDI Client installation program checks to ensure that either the Citrix Receiver or the VMware Horizon Client is already installed on the reused PC. In one of the following registry locations, the `InstallFolder` string-type registry key must be present:

- For Citrix, the installer searches in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Instal\ICA Client` for the path to the Citrix installation.

Example (from an x86 PC): [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Install\ICA Client] "InstallFolder"="C:\\Program Files\\Citrix\\ICA Client\\"

- For VMware Horizon, the installer searches in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM for the path to the VMware installation.

Example (from an x64 PC): [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM] "ClientInstallPath"="C:\\Program Files\\VMware\\VMware View\\Client\\"

Verify That Cisco JVDI Client Is Running

Use Windows Task Manager to verify that Cisco JVDI Client is running.

In a Citrix environment, the Cisco Jabber Softphone for VDI processes start when the user signs in to their hosted virtual desktop (HVD). The processes stop when the session ends.

In a VMware environment, the Cisco Jabber Softphone for VDI processes start after the user signs in to their HVD and in to Cisco Jabber. The processes stop when the session ends.

-
- Step 1** On the thin client desktop, right-click the taskbar and then select **Task Manager**.
- Step 2** On the **Processes** tab, scroll down and look for the vxc.exe process.
-

Confirm the Version of Cisco JVDI Client

Cisco JVDI Client appears in the list of installed programs and features.

-
- Step 1**
- Step 2** On the thin client, open **Control Panel > Programs and Features**.
- Step 3** Scroll down the list and locate Cisco JVDI Client.
- Step 4** To confirm the version for Cisco JVDI Client, see the **Version** column.
-

Call Control Is Lost After a Network Failure

Users see a prompt to reconnect to their hosted virtual desktops (HVDs). After the users reconnect, Cisco Jabber call control features do not work.

This problem can occur if the thin client loses network connectivity.

To resolve this issue, have the users exit Cisco Jabber and disconnect from their HVDs. Next they can log back in to their HVDs and sign back in to Cisco Jabber to restore call control.

Call Is Lost After HVD Disconnection

Users receive a prompt to log back in to their hosted virtual desktops (HVD) during an active call, and the call drops. The other party to the call has no indication that the call has ended, except the line is silent.

This issue can occur if the connection between the thin client and the HVD drops, causing a temporary loss of registration and call control.

To work around this issue, users can call the other party back. If the other party is not available, users can send an instant message (IM).

Enable Log Collection

You can modify the Cisco configuration file (cisco.conf) to enable the collection of logs from the thin client.

The cisco.conf file is located in: C:\Program Files (x86)\Cisco Systems\Cisco VXME\cisco.conf

Step 1 Open the cisco.conf file and add the following lines:

```
[logger]
log_level = Debug
```

You can set the log level to one of the following values: Fatal, Error, Warning, Info, Debug or Trace. The default level is Debug.

Step 2 Save the file.

Step 3 Restart the vxc process by logging out and back in to the HVD.

Enable Memory Dump Collection

You can modify the Cisco configuration file (cisco.conf) to enable the Problem Reporting Tool (PRT) to collect a memory dump.

For Windows 32-bit, the cisco.conf file is located in C:\Program Files (x86)\Cisco Systems\Cisco VXME\cisco.conf.

For Windows 64-bit, the cisco.conf file is located in C:\Program Files\Cisco Systems\Cisco VXME\cisco.conf.

Step 1 Open the cisco.conf file and add the following lines:

```
[logger]
dump_type = Minidump
dump_when_collect_log = True
```

You can set the `dump_type` to `Fulldump` or `Minidump`. The default is `Minidump`. If `dump_when_collect_log` is set to `False`, the PRT doesn't collect the memory dump.

- Step 2** Save the file.
 - Step 3** Restart the `vxc` process by logging out and back in to the HVD.
-

Display issues

Certain third-party application window can make preview, remote video, and remote share display as gray when the window is close to a Jabber conversation window ([CSCvz75206](#)).

In Jabber Softphone for VDI Release 14.0.3, we added support for a new Jabber parameter, **EnableVDIFullScan**, to correct these issues. You must run JVDI 14.0.3 with Jabber for Windows 14.0.4 to use this parameter.